Worksheet Instructions for:
Evaluating Controls over Automated Information Systems
"General Controls"

General Instructions and Considerations

Due to the formation of the Department of Information Technology (DIT), many IT related responsibilities that were formerly assumed by agency/department Management has shifted to Department of Information Technology (DIT) management. DIT management is responsible for the State of Michigan's General Controls environment, while agency management are the business process/application owners and, therefore, hold responsibility for managing their Application Specific Controls and their Application Environment Controls. As part of the ongoing evaluation of internal controls and the biennial internal control evaluation reporting process, DIT management developed a "General Controls" worksheet to document controls over the Statewide general IT environment. In addition, worksheets exist for business process owners to evaluate "Application Specific" and "Application Environment" controls. These evaluation tools are essential for departments responsible for administering critical information systems that support departmental business processes.

CobiT (Control Objectives for Information and Related Technology), developed by the Information Systems Audit and Control Foundation (ISACF), was used as a foundation in preparing the General Controls, Application Specific Controls and Application Environment Controls worksheets. CobiT is designed for use by IT management/users and information systems auditors, and is considered one of the most effective and widely accepted tools for evaluating security and control in the IT environment.

"General Controls" relate to activities that provide for the proper operation of application systems. General controls encompass strategic planning, business continuity, contingency planning, system development methodology, procedures for documenting, reviewing, testing, and approving system changes, and a variety of other control activities. More specific instructions for utilizing the General Controls worksheets (doc) (pdf) are provided below.

"Application Environment" controls (instructions (doc) (pdf), worksheets (doc) (pdf)) relate to the environment in which the agency's various computer applications reside. Controls are focused toward service level agreements, data storage and back up, end user support, and others. If controls over the application environment are the same across all agency applications, the worksheet will only need to be completed once.

"Application Specific" controls (instructions (doc) (pdf), worksheets (doc) (pdf)) focus on input, processing, and output controls over the application. These controls should be evaluated for each application that the agency deems critical to accomplish their business objectives.

Collaboration between IT personnel and non-IT activity managers is necessary to evaluate risks/controls over the objectives listed on the worksheet(s).

It is critical to document the agency's internal control structure/systems, in addition to evaluating the control structure. In past biennial evaluations, documentation efforts have not been sufficiently addressed, particularly for each department's unique IT environment. Improved documentation will reduce efforts/resources required to complete the next biennial evaluation and facilitate periodic monitoring of controls by managers of the information systems.

(You may customize the worksheet during the evaluation process to meet your specific needs or if using it for the first time, but the standard worksheet is recommended.)

Specific Instructions

In preparation for evaluating the general controls over the State's IT environment, you may wish to determine if other reviews of information systems and data center operations have been conducted recently. When obtaining assurances about the effectiveness of general computer and application controls in the IT environments being evaluated, utilize reviews/audits conducted by the Auditor General, internal evaluations, Statements of Auditing Standards (SAS) 70 reviews, consulting engagements, etc. **Attach such documentation, if used in completion of this evaluation worksheet.**

There is one worksheet to be used when evaluating general controls over the State's IT environment. This worksheet is entitled "Evaluating General Controls over Automated Information Systems" and should be used to evaluate controls related to the entire environment in which the Department's/Agency's various computer applications reside. The worksheet is segregated into four (4) primary domains: Planning and Organization (PO), Acquisition and Implementation (AI), Delivery and Support (DS), and Monitoring (M). Within the four domains, there are 34 high-level IT processes identified. Each IT Process has an associated control objective, which will need to be evaluated to determine if adequate controls are in place to meet that control objective. In addition to the worksheet, it will be necessary for the individuals completing the worksheet to refer to the detailed CobiT control objectives document. The control objectives document contains statements of the desired results or purposes to be achieved by implementing specific control procedures within an IT Process.

The columns within the worksheet are described as follows:

- *IT Process (Column 1)* – Identifies each component (IT process) at the level that the Department should evaluate and document existing controls in respective IT processes and environments.

- *Risks (Column 2)* - Identifies potential risks that may result from a lack of appropriate policies, procedures and/or controls over the IT Process identified in column 1.

- *Objective (Column 3)* - Summarizes typical elements of a management and control structure that would address risks applicable to each IT Process. Reference is made to detailed control objectives within the CobiT-Control Objectives document that should be met to satisfy the identified IT Process (for example, control objectives PO 1.1-1.6 should be met to satisfy the IT Process PO 1.0, which is to Define a Strategic IT Plan).

  (Use remaining worksheet columns to document assessment of actual internal controls within each IT environment.)

- *Responsible Activity (Column 4)* - Identify the activity (e.g., Agency, Division, Office, and/or Staff within DIT) responsible for each IT Process, particularly when noting specific processes in later columns as being not applicable to the responsible activity completing the worksheet.

- *Columns 5-12* – Enter check marks to denote whether appropriate controls (see Column 3) exist within the IT environment being evaluated; and whether controls are documented, effective, and sufficient.

Existence:

D - Documented
ND - Not Documented
N/A - Not Sure or Not Applicable

Performance/Effectiveness:

E - Excellent
V - Very Good
S - Satisfactory
I - Ineffective/Insufficient
N/A - Not Sure or Not Applicable

NOTE: When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements

- *Description/Comments (Column 13)* - Enter description/comments related to information and conclusions made in previous columns; identify formal policies, procedures, and informal practices that represent internal controls related to the IT Process. Identify, at a minimum, control objectives for which appropriate control activities do not currently exist, whether there are alternative or compensating controls, and whether plans and time frames exist for addressing deficiencies in the control structure.

  NOTE: Attach a supplemental sheet if you are not able to fit all relevant information in this column